INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-05 08:18 UTC

Dual-RMM Persistence Campaign (VENOMOUS#HELPER / STAC6405) Targets 80+ U.S. Organizations via SSA Phishing

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0271
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	SimpleHelp 5.0.1, ConnectWise ScreenConnect, Windows (JWrapper-packaged executable, Windows services, WMI SecurityCenter2 namespace)
Published	2026-05-04T14:06:00
Discovery Source	Rss

Executive Summary

An active phishing campaign impersonating the U.S. Social Security Administration has compromised more than 80 U.S. organizations by deploying two remote access tools simultaneously, with watchdog and Safe Mode persistence mechanisms designed to re-establish access if one channel is removed. The attackers gain SYSTEM-level control over Windows endpoints, a profile consistent with ransomware precursor operations. Organizations running SimpleHelp 5.0.1 or ConnectWise ScreenConnect are at elevated risk of sustained compromise, data theft, and ransomware deployment.

Technical Analysis

Campaign designations: VENOMOUS#HELPER / STAC6405. Initial access is via spearphishing links (T1566.002) and attachments (T1566.001) impersonating SSA communications. The lure delivers a JWrapper-packaged Windows executable that installs SimpleHelp 5.0.1 and ConnectWise ScreenConnect as dual redundant C2 channels (T1219). The payload registers as a Windows service (T1543.003) with Safe Mode persistence (T1547.001) and escalates to SYSTEM via AdjustTokenPrivileges / token manipulation (T1134, T1548.002). A watchdog process monitors and restores removed components. The malware queries WMI SecurityCenter2 namespace to enumerate installed security products (T1518.001) and may enumerate running processes (T1057) to identify security monitoring agents. Suppression occurs via masquerading (T1036.005) and virtualization/sandbox evasion (T1497). Registry modifications (T1112) support persistence. Remote services (T1021, T1021.001) are used for lateral movement post-access, potentially using compromised valid

accounts (T1078). Threat actor acquires infrastructure via virtual private servers (T1583.003). No CVE is assigned to this campaign. The attack relies on social engineering (SSA phishing) to trick users into installing legitimate RMM software, not on exploiting a software vulnerability in SimpleHelp or ScreenConnect. (Note: Both tools may have published vulnerabilities independent of this campaign; this campaign's success does not depend on those vulnerabilities.) Relevant CWEs: CWE-693 (Protection Mechanism Failure), CWE-732 (Incorrect Permission Assignment), CWE-269 (Improper Privilege Management). No CISA KEV entry as of configuration date. Source quality is T3 (secondary news and community sources); primary vendor advisories from SimpleHelp and ConnectWise were not available in the provided source set.

Action Checklist

1. Containment: Audit all Windows endpoints for unauthorized SimpleHelp 5.0.1 and ConnectWise ScreenConnect installations not provisioned by your IT or MSP team. Isolate any host where unrecognized RMM software is found. Block outbound connections to SimpleHelp and ScreenConnect relay infrastructure at the perimeter for hosts not authorized to use these tools.
2. Detection: Search endpoint logs and EDR telemetry for: new Windows services registered by JWrapper-packaged executables; AdjustTokenPrivileges token manipulation events (Windows Security Event ID 4672, 4673); WMI queries targeting the SecurityCenter2 namespace; processes restarting deleted or stopped services (watchdog behavior). Review email gateway logs for SSA-themed lures with executable links or attachments delivered to U.S. staff.
3. Eradication: Remove unauthorized SimpleHelp and ScreenConnect installations from all affected endpoints. Delete associated Windows services, registry run keys (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and equivalent Safe Mode keys), and scheduled tasks created by the installer. Verify removal persists through a reboot into Safe Mode and back to normal boot, using WMI or registry monitoring to confirm no service or key re-creation occurs, before clearing the host as remediated.
4. Recovery: Re-image confirmed compromised hosts where SYSTEM-level access was achieved; do not trust in-place remediation alone for hosts with confirmed privilege escalation. Reset all credentials that may have been exposed on affected systems (local accounts, domain accounts used interactively, service accounts). Monitor for re-infection via the same SSA phishing vector for 30 days post-remediation.
5. Post-Incident: Review email filtering controls for executable-delivering lures impersonating U.S. government agencies. Implement an explicit allowlist policy for RMM tools: only approved, IT-provisioned RMM software should be permitted to run and communicate externally. Evaluate Safe Mode protection controls, consider solutions that enforce EDR persistence through Safe Mode boot. Map gaps to MITRE ATT&CK T1219 (Remote Access Software) and T1543.003 (Windows Service) detection coverage.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership and legal/compliance counsel immediately if any affected host is confirmed to have achieved SYSTEM-level access with evidence of lateral movement, credential harvesting, or data staging activity, as this campaign's ransomware-precursor profile and 80+ organization blast radius may trigger state breach notification obligations or sector-specific regulatory reporting (e.g., HIPAA, GLBA) depending on data exposed on compromised endpoints.
Recovery Notes	Re-imaging is required — not optional — for any host where SYSTEM-level privilege escalation is confirmed, as the dual-RMM redundancy mechanism (SimpleHelp plus ScreenConnect with Safe Mode persistence) means partial removal leaves a functional attacker foothold. Post-reimaging, monitor all previously affected hosts and adjacent systems for 30 days specifically for re-deployment of JWrapper-packaged executables (Sysmon Event ID 7045, new service installs) and renewed outbound connections to SimpleHelp or ScreenConnect relay infrastructure. Verify that Safe Mode registry persistence keys under `HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\` remain clean on all remediated hosts throughout the monitoring window.
Forensic Artifacts	Windows System Event Log (Event ID 7045 — New Service Installed): Records the registration of JWrapper-packaged SimpleHelp and ScreenConnect services by name, ImagePath pointing to non-standard directories (AppData, Temp, ProgramData), and the SYSTEM or admin account context used — this is the primary evidence of dual-RMM service persistence specific to this campaign. | Registry keys HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal and \Network: This campaign specifically abuses Safe Mode boot persistence by inserting RMM service names into these keys, ensuring the backdoor survives EDR-assisted Safe Mode remediation attempts — export and hash these keys on all potentially affected hosts. | WMI Repository (C:\Windows\System32\wbem\Repository\): The campaign queries the SecurityCenter2 namespace to identify and evade registered AV/EDR products — forensic analysis of the WMI repository and Sysmon WMI activity logs (Event IDs 19, 20, 21) will show attacker enumeration of security tool visibility before deploying RMM payloads. | Email gateway delivery logs with JWrapper/.jnlp/.jar attachment or link metadata: The SSA-impersonation phishing lure is the initial access vector — preserving full SMTP headers, envelope-from, originating IP, and the exact download URL for the JWrapper executable enables attribution, IOC extraction, and email rule development to block re-delivery to the remaining ~80 affected organizations. | Prefetch files (C:\Windows\Prefetch\) and Shimcache / Amcache registry hives: These artifacts record first and last execution timestamps for the JWrapper installer and both RMM binaries even after the files are deleted, providing execution timeline evidence that survives partial eradication attempts and supports determination of the initial compromise date.

Per-Action IR Details

Containment — Audit all Windows endpoints for unauthorized SimpleHelp 5.0.1 and ConnectWise ScreenConnect installations not provisioned by your IT or MSP team. Isolate any host where unrecognized RMM software is found. Block outbound connections to SimpleHelp and ScreenConnect relay infrastructure at the perimeter for hosts not authorized to use these tools.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 2.3 (Address Unauthorized Software)

Compensating: Run the following PowerShell on each endpoint to detect SimpleHelp and ScreenConnect installations: `Get-WmiObject Win32_Product | Where-Object { $_.Name -match 'SimpleHelp|ScreenConnect|ConnectWise' }` and `Get-Service | Where-Object { $_.DisplayName -match 'SimpleHelp|ScreenConnect|JWrapper' }`. Cross-reference against your IT-provisioned RMM allowlist. For perimeter blocking without enterprise tooling, add egress ACL rules on your edge firewall/router to block outbound TCP 443/80 to known SimpleHelp relay domains (e.g., *.simplehelp.net) and ScreenConnect relay infrastructure (*.screenconnect.com) for all hosts not on the RMM-authorized asset list. Use Sysmon Event ID 3 (Network Connection) to identify hosts actively beaconing to these domains before isolation.

Evidence: Before isolating any host, capture: (1) full process list with parent-child relationships via `Get-Process` and `wmic process get name,processid,parentprocessid,executablepath`; (2) active network connections via `netstat -anob` to document live C2 sessions to SimpleHelp/ScreenConnect relay IPs; (3) installed services list via `sc query type= all state= all`; (4) JWrapper executable file hash from the installation path (typically `C:\Program Files\SimpleHelp\` or user-writable temp directories) for IOC correlation; (5) prefetch files (`C:\Windows\Prefetch\`) for execution evidence of the phishing-delivered JWrapper installer.

Detection — Search endpoint logs and EDR telemetry for: new Windows services registered by JWrapper-packaged executables; AdjustTokenPrivileges token manipulation events (Windows Security Event ID 4672, 4673); WMI queries targeting the SecurityCenter2 namespace; processes restarting deleted or stopped services (watchdog behavior). Review email gateway logs for SSA-themed lures with executable links or attachments delivered to U.S. staff.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, deploy Sysmon with SwiftOnSecurity's config (https://github.com/SwiftOnSecurity/sysmon-config) and query collected .evtx files using `Get-WinEvent`. Specific queries: (1) For JWrapper service registration — query Windows System Event Log for Event ID 7045 (New Service Installed) filtering on ImagePath containing 'JWrapper' or 'SimpleHelp' or temp directory paths: `Get-WinEvent -LogName System | Where-Object { $_.Id -eq 7045 -and $_.Message -match 'JWrapper|SimpleHelp|AppData|Temp' }`; (2) For token privilege abuse — query Windows Security Event Log for Event IDs 4672 (Special Logon) and 4673 (Sensitive Privilege Use) filtering on SeDebugPrivilege or SeTcbPrivilege; (3) For WMI SecurityCenter2 queries — query Sysmon Event ID 19/20/21 (WMI Activity) for queries containing 'SecurityCenter2'; (4) For watchdog restarts — look for Sysmon Event ID 1 (Process Create) where a child process image matches a known RMM binary restarting within 60 seconds of a stop event. For email gateway, export MTA logs and grep for SSA-themed subject lines: `grep -i 'social security\|ssa.gov\|benefit\|retirement' mail.log`.

Evidence: Preserve before analysis: (1) Windows Security Event Log (.evtx) from affected hosts, specifically filtering Event IDs 4672, 4673, 4688 (Process Creation) for JWrapper-spawned processes and SYSTEM-context events; (2) Sysmon operational log capturing Event ID 1 entries showing the JWrapper executable's full command line and parent process (likely browser or email client for the initial phish delivery); (3) WMI repository (`C:\Windows\System32\wbem\Repository\`) snapshot to document SecurityCenter2 namespace tampering used to suppress AV visibility; (4) Email gateway delivery logs showing originating IP, envelope-from, and any URL or attachment metadata for the SSA-impersonation lure; (5) Windows Application Event Log entries from the JWrapper runtime showing installation activity timestamps for timeline reconstruction.

Eradication — Remove unauthorized SimpleHelp and ScreenConnect installations from all affected endpoints. Delete associated Windows services, registry run keys (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and equivalent Safe Mode keys), and scheduled tasks created by the installer. Verify removal persists through reboot, including Safe Mode boot, before clearing the host.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For Safe Mode persistence removal without EDR: (1) Check and delete Safe Mode registry run keys that survive standard boot: `reg query 'HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal' /s` and `reg query 'HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network' /s` — remove any entries referencing SimpleHelp, ScreenConnect, or JWrapper service names; (2) Remove associated services: `sc delete ` for each unauthorized RMM service identified; (3) Delete scheduled tasks: `schtasks /query /fo LIST /v | findstr /i 'simplehelp screenconnect jwrapper'` then `schtasks /delete /tn /f`; (4) After removal, reboot into Safe Mode manually (bcdedit /set safeboot minimal) and run `sc query type= all state= all` again to confirm the service does not reload; (5) Restore normal boot with `bcdedit /deletevalue safeboot` after verification. Use Sysinternals Autoruns (free) to visualize all persistence mechanisms in a single view before and after removal.

Evidence: Before eradication, image or capture: (1) Registry export of `HKLM\SYSTEM\CurrentControlSet\Services\` subtree covering all JWrapper/SimpleHelp/ScreenConnect service entries including their ImagePath, Start type, and any watchdog-related parameters; (2) Full export of `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, `RunOnce`, and Safe Mode equivalents under `HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\`; (3) Scheduled task XML exports via `schtasks /query /xml` capturing any tasks created by the RMM installer with creation timestamps; (4) File system snapshot of RMM installation directories and any dropped payloads in `%APPDATA%`, `%TEMP%`, or `C:\ProgramData\` for malware triage; (5) Memory acquisition (via WinPmem, free) if SYSTEM-level access is confirmed, to capture any in-memory payloads or credentials prior to service termination.

Recovery — Re-image confirmed compromised hosts where SYSTEM-level access was achieved; do not trust in-place remediation alone for hosts with confirmed privilege escalation. Reset all credentials that may have been exposed on affected systems (local accounts, domain accounts used interactively, service accounts). Monitor for re-infection via the same SSA phishing vector for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST IA-5 (Authenticator Management), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For re-image verification without enterprise tooling: (1) After re-imaging from a known-good baseline, run `sfc /scannow` and verify OS integrity; (2) Validate no SimpleHelp or ScreenConnect binaries persist using: `Get-ChildItem -Path C:\ -Recurse -Include 'SimpleHelp*','ScreenConnect*','JWrapper*' -ErrorAction SilentlyContinue`; (3) For credential reset scope determination, extract Windows Security Event ID 4624 (Successful Logon) and 4648 (Explicit Credential Use) from the compromised host's preserved logs to identify every account that authenticated during the compromise window — reset all of them; (4) For 30-day re-infection monitoring without EDR, configure Sysmon to alert on Event ID 7045 (New Service Installed) and route to a central log file reviewed daily; deploy a Sigma rule for JWrapper service installation patterns using sigmac to convert to native Windows Event Log queries.

Evidence: Before re-imaging, preserve for post-incident use: (1) Full disk image of compromised hosts (use FTK Imager Lite, free) to support any later forensic analysis or legal hold requirements, particularly given potential ransomware precursor activity across 80+ organizations; (2) Active Directory logs showing any lateral movement from compromised endpoints — query Domain Controller Security Event Log for Event ID 4768/4769 (Kerberos ticket requests) and 4624 Type 3 (network logons) originating from affected hosts during the compromise window; (3) Service account usage logs to establish whether accounts with elevated domain privileges were used interactively on compromised hosts; (4) Captured network flows or firewall logs documenting all outbound connections made by the RMM tools during the active compromise period for IOC extraction.

Post-Incident — Review email filtering controls for executable-delivering lures impersonating U.S. government agencies. Implement an explicit allowlist policy for RMM tools: only approved, IT-provisioned RMM software should be permitted to run and communicate externally. Evaluate Safe Mode protection controls — consider solutions that enforce EDR persistence through Safe Mode boot. Map gaps to MITRE ATT&CK T1219 (Remote Access Software) and T1543.003 (Windows Service) detection coverage.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-3 (Malicious Code Protection), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For teams without enterprise email security: (1) Create email gateway rules blocking .exe, .jar, and .jnlp attachments (JWrapper uses Java Web Start delivery vectors) and flag messages with display names containing 'Social Security Administration', 'SSA', or 'ssa.gov' that originate from non-.gov sending domains; (2) Build an RMM allowlist policy using Windows AppLocker (built-in, free) or Software Restriction Policies — whitelist only the hash or publisher certificate of your IT-approved RMM binary and block all others including SimpleHelp and ScreenConnect if not provisioned by your team; (3) For MITRE T1219 and T1543.003 detection coverage gaps, download and deploy Sigma rules from the SigmaHQ repository (https://github.com/SigmaHQ/sigma) — specifically rules tagged with T1219 and T1543.003 — and convert them to Windows Event Log queries using the free sigmac tool; (4) Document the incident and gaps in a lessons-learned report per NIST 800-61r3 §4 to drive IR plan updates for dual-RMM persistence scenarios.

Evidence: Collect for lessons-learned and detection tuning: (1) Complete email header and body samples of the SSA-impersonation phishing lures received, including the original JWrapper executable download URL, to build organization-specific YARA rules and email gateway signatures; (2) All unique hashes (MD5/SHA-256) of SimpleHelp 5.0.1 and ScreenConnect installer binaries dropped during this campaign, cross-referenced against VirusTotal for existing detection coverage; (3) Network IOC list — all C2 relay IPs and domains contacted by the RMM tools during active compromise, sourced from captured netflow/firewall logs, for perimeter block-list and threat intelligence sharing; (4) Timeline of the full attack chain from phish delivery through SYSTEM-level access establishment, mapped to MITRE ATT&CK T1219 and T1543.003, to identify where existing controls failed and where new detections must be placed.

Detection Guidance

Priority detection signals: (1) Windows Service Creation, Event ID 7045 (System log) for services with JWrapper-style naming conventions or unusual binary paths pointing to user-writable directories. (2) Token Privilege Abuse, Event IDs 4672 and 4673 (Security log) for AdjustTokenPrivileges calls from non-standard processes. (3) WMI SecurityCenter2 Enumeration, Monitor WMI activity logs (Microsoft-Windows-WMI-Activity/Operational, note: enable this log if not already configured in Event Viewer) for queries to ROOT\SecurityCenter2 from unexpected processes. (4) RMM Dual-Channel Behavior, Network detections for simultaneous outbound SimpleHelp relay and ScreenConnect relay connections from the same host. (5) Safe Mode Persistence, Registry monitoring for modifications to HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal or Network keys adding non-OS services. (6) Watchdog Process Pattern, EDR process tree analysis for parent processes that respawn child processes immediately after termination. (7) Phishing Entry Point, Email gateway alerts for SSA-themed messages containing links to executable downloads or ZIP attachments containing JWrapper executables. Behavioral hunting hypothesis: identify any host running both SimpleHelp and ScreenConnect concurrently where neither was provisioned through change management.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	[not published in available sources]	SimpleHelp and ScreenConnect relay infrastructure used for dual C2 — specific domains not disclosed in T3 sources reviewed	LOW
HASH	[not published in available sources]	JWrapper-packaged executable hash not disclosed in T3 sources reviewed	LOW

Framework Mappings

MITRE-ATTACK

- **T1518.001** — Security Software Discovery
- **T1543.003** — Windows Service
- **T1057** — Process Discovery
- **T1583.003** — Virtual Private Server
- **T1566.002** — Spearphishing Link
- **T1112** — Modify Registry
- **T1548.002** — Bypass User Account Control
- **T1105** — Ingress Tool Transfer
- **T1082** — System Information Discovery
- **T1021** — Remote Services
- **T1021.001** — Remote Desktop Protocol
- **T1497** — Virtualization/Sandbox Evasion
- **T1078** — Valid Accounts
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1566.001** — Spearphishing Attachment
- **T1219** — Remote Access Tools
- **T1134** — Access Token Manipulation

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-7** — Continuous Monitoring
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement

- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **3.3** — Configure Data Access Control Lists
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1518.001	Security Software Discovery	Discovery
T1543.003	Windows Service	Persistence
T1057	Process Discovery	Discovery
T1583.003	Virtual Private Server	Resource-Development
T1566.002	Spearphishing Link	Initial-Access
T1112	Modify Registry	Defense-Evasion

Technique ID	Technique Name	Tactic
T1548.002	Bypass User Account Control	Privilege-Escalation
T1105	Ingress Tool Transfer	Command-And-Control
T1082	System Information Discovery	Discovery
T1021	Remote Services	Lateral-Movement
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1497	Virtualization/Sandbox Evasion	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1566.001	Spearphishing Attachment	Initial-Access
T1219	Remote Access Tools	Command-And-Control
T1134	Access Token Manipulation	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/phishing-campaign-hits-80-orgs-us...	T3
Connectwise Cloud Hosted ScreenConnect Detected as Virus ...	https://www.reddit.com/r/ScreenConnect/comments/1r25k71/connectwise...	T3
CISA Warning: Attacks on ConnectWise ScreenConnect and ... - Heise	https://www.heise.de/en/news/CISA-Warning-Attacks-on-ConnectWise-Sc.. .	T3
Responding to the ScreenConnect Vulnerability - ConnectWise	https://www.connectwise.com/blog/responding-to-screenconnect-vulner...	T3
Potential Vulnerability with simplehelp install - Remote Support and ...	https://community.simple-help.com/t/potential-vulnerability-with-si...	T3

Generated 2026-05-05 08:18 UTC by TJS Security Command Center